PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-191787
(43)Date of publication of application : 10.07.1992

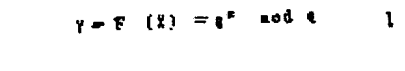
(51)Int.Cl. G09C 1/00
G06F 12/14
H04L 9/28

(21)Application number : 02-324479
(22)Date of filing : 26.11.1990

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HARADA TOSHIHARU
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(54) DISCLOSURE KEY PRODUCING METHOD AND DISCLOSURE KEY GENERATING SYSTEM

(57)Abstract:
PURPOSE: To omit the step for completeness confirmation of a disclosure key by adapting a method for not conducting the completeness confirmation of a disclosure value independently, and conducting the completeness confirmation of the disclosure value simultaneously with the authorization of a partner terminal.



CONSTITUTION: A large prime number or the power multiplier of the prime number (q) and the primitive element (g) of GF (q) are generated, and the (q) and (g) are stored in a modulus storing part 11 and a primitive element storing part 12, respectively. The secret key X of a center is determined and stored in a secret key storing part 13, and the secret key X of the center is inputted to an unidirectional function F:14 to generate an expression I. The (q), (g), V of the expression I and a disclosure key producing function P used in the disclosure key producing step are disclosed to each terminal as the disclosure information of the center. The terminal (i) notifies the center of the identification information IDi inherent to the terminal (i) stored in an identification information storing part 21 through a communication passage 41 for claiming the terminal information and claims the issue of the terminal information. The center confirms the validity of the terminal (i) and generates a random number Ki by a random number producing device 15, inputs this value to the unidirectional function 14 to produce the disclosure value of the terminal, and issues it to the terminal through a terminal information issuing passage.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－191787

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成4年(1992)7月10日
G 09 C 1/00		7922－5L	
G 06 F 12/14	320 B	8841－5B	
H 04 L 9/28			
		7117－5K　H 04 L 9/02	A

審査請求　未請求　請求項の数 8　（全13頁）

⑭発明の名称　公開鍵生成方式および公開鍵生成システム

⑳特　願　平2－324479
㉒出　願　平2(1990)11月26日

⑫発明者	原田　俊治	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑫発明者	松崎　なつめ	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑫発明者	館林　誠	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑪出願人	松下電器産業株式会社	大阪府門真市大字門真1006番地	
⑭代理人	弁理士　中島　司朗		

明　細　書

1.発明の名称

公開鍵生成方式および公開鍵生成システム

2.特許請求の範囲

(1) 固有の識別情報を有する第1の端末と第2の端末とこれらを含むネットワークと端末情報発行センターで構成されるシステムにおいて、

前記端末情報発行センターが、センターの秘密鍵Xと、端末の秘密鍵を生成するためのある秘密鍵生成関数Sを有し、端末の公開鍵を生成するためのある公開鍵生成関数Pと、ある一方向性関数Fと、前記センターの秘密鍵Xを前記一方向性関数Fに入力したときの出力値Y＝F（X）を、センターの公開情報として、前記第1および第2の端末に通知するシステム初期設定ステップと、

前記第1の端末が、第1の端末固有の識別情報iを前記端末情報発行センターに通知し、前記第1の端末の端末情報として、前記第1の端末の秘密鍵と公開値の発行を請求する端末情報請求ステップと

前記第1の端末からの端末情報発行請求を受けた前記端末情報発行センターが、前記第1の端末の公開値として、ある乱数値kを前記一方向性関数Fに入力したときの出力値y＝F（k）を生成し、前記第1の端末の秘密鍵として、前記センターの秘密鍵Xと、前記第1の端末の公開値yと、前記乱数値kと、前記第1の端末の識別情報iを前記秘密鍵生成関数Sに入力したときの出力値

x＝S（X，y，k，i）

を生成し、前記第1の端末の公開値yと、前記第1の端末の秘密鍵xを前記第1の端末の端末情報として発行する端末情報発行ステップと、

前記端末情報発行センターから端末情報の発行を受けた前記第1の端末が、前記第2の端末に対して、前記第1の端末の公開情報として、前記第1の端末の公開値yと識別情報iを、前記通信ネットワークを介して転送する端末公開情報転送ステップと、

前記第1の端末から前記端末公開情報の転送を受けた前記第2の端末が、前記第1の端末の公開

鍵として、前記センターの公開情報Ｙと、前記第１の端末の公開値ｙと、前記第１の端末の識別情報ｉを前記公開鍵生成関数Ｐに入力したときの出力値

Ｃ＝Ｐ（Ｙ，ｙ，ｉ）

を生成する公開鍵生成ステップから構成されることを特徴とした公開鍵生成方式。

(2) 請求項１記載の公開鍵生成方式において、ｑを素数もしくは素数のべき乗値とし、ｇを前記ｑを法とする剰余体の原始元とし、ｕを前記剰余体のある元としたとき、前記一方向性関数Ｆとして、前記ｑを法とし、前記ｕを入力とする前記ｇのべき乗剰余値

ｖ＝Ｆ（ｕ）＝g^u mod q

を出力する関数を使用し、φを前記ｑのオイラー関数値としたとき、前記秘密鍵生成関数Ｓとして、前記φを法とし、センターの秘密鍵Ｘと第１の端末の公開値ｙの積と、センターの生成した乱数値ｋと第１の端末の識別情報ｉの積との和

ｘ＝Ｓ（Ｘ，ｙ，ｋ，ｉ）

＝Ｘ×ｙ＋ｋ×ｉ　mod φ

を出力する関数を使用し、前記公開鍵生成関数Ｐとして、前記ｑを法とし、前記第１の端末の公開値ｙをべきとした前記センターの公開情報Ｙのべき乗剰余値と、前記第１の端末の識別情報ｉをべきとした前記第１の端末の公開値ｙのべき乗剰余値との積

Ｃ＝Ｐ（Ｙ，ｙ，ｉ）

＝$(Y^y) \times (y^i)$ mod q

を出力する関数を使用することを特徴とする公開鍵生成方式。

(3) 請求項１記載の公開鍵生成方式において、ｑを素数もしくは素数のべき乗値とし、ｇを前記ｑを法とする剰余体の原始元とし、ｕを前記剰余体のある元としたとき、前記一方向性関数Ｆとして、前記ｑを法とし、前記ｕを入力とする前記ｇのべき乗剰余値

ｖ＝Ｆ（ｕ）＝g^u mod q

を出力する関数を使用し、φを前記ｑのオイラー関数値としたとき、前記秘密鍵生成関数Ｓとして、前記φを法とし、前記第１の端末の公開値ｙと前記第１の端末の識別情報ｉをある公開の関数Ｈに入力したときに得られる出力値ｈと、前記センターの秘密鍵Ｘの積と、前記センターの生成した乱数値ｋとの和

ｘ＝Ｓ（Ｘ，ｙ，ｋ，ｉ）

＝Ｈ(y,i)×Ｘ＋ｋ mod φ

＝ｈ×Ｘ＋ｋ　mod φ

を出力する関数を使用し、前記公開鍵生成関数Ｐとして、前記ｑを法とし、前記第１の端末の公開値ｙと前記第１の端末の識別情報ｉを前記関数Ｈに入力したときに得られる出力値ｈをべきとした前記センターの公開情報Ｙのべき乗剰余値と、前記第１の端末の公開値ｙとの積

Ｃ＝Ｐ（Ｙ，ｙ，ｉ）

＝$(Y^{H(y,i)}) \times y$ mod q

＝$(Y^h) \times y$ mod q

を出力する関数を使用することを特徴とする公開鍵生成方式。

(4) 請求項１記載の公開鍵生成方式であって、前記端末情報の発行ステップの後に、前記第１の端末が、検証用公開鍵として、前記第１の端末の秘密鍵ｘを前記一方向性関数Ｆに入力したときの出力値Ｖ＝Ｆ（ｘ）を生成する検証用公開鍵生成ステップを追加し、

前記端末公開情報転送ステップにおいて、前記第１の端末が、前記第２の端末に、前記検証用公開鍵Ｖと、前記第１の端末の識別情報ｉと、前記第１の端末の公開値ｙを、前記第１の端末の公開情報として前記通信ネットワークを介して転送し、

前記第１の端末から端末公開情報の転送を受けた前記第２の端末が、前記公開鍵生成ステップの後に、前記公開鍵生成ステップで生成された前記第１の端末の公開鍵Ｃと前記検証用公開鍵Ｖを比較し、一致するか否かを確認する公開鍵確認ステップを追加することを特徴とした公開鍵生成方式。

(5) 固有の識別情報を有する第１の端末と第２の端末とこれらを含むネットワークと端末情報発行センターで構成されるシステムであって、

前記端末情報発行センターは、センターの秘密鍵Xと、端末の秘密鍵を生成するためのある秘密鍵生成関数Sを有し、端末の公開鍵を生成するためのある公開鍵生成関数Pと、ある一方向性関数Fと、前記センターの秘密鍵Xを前記一方向性関数Fに入力したときの出力値Y＝F（X）を、センターの公開情報として、前記第1および第2の端末に通知するシステム初期設定部と、

前記第1の端末は、第1の端末固有の識別情報iを前記端末情報発行センターに通知し、前記第1の端末の端末情報として、前記第1の端末の秘密鍵と公開値の発行を請求する端末情報請求部と、

前記第1の端末からの端末情報発行請求を受けた前記端末情報発行センターが、前記第1の端末の公開値として、ある乱数値kを前記一方向性関数Fに入力したときの出力値y＝F（k）を生成し、前記第1の端末の秘密鍵として、前記センターの秘密鍵Xと、前記第1の端末の公開値yと、前記乱数値kと、前記第1の端末の識別情報iを前記秘密鍵生成関数Sに入力したときの出力値

$$x = S(X, y, k, i)$$

を生成し、前記第1の端末の公開値yと、前記第1の端末の秘密鍵xを前記第1の端末の端末情報として発行する端末情報発行部と、

前記端末情報発行センターから端末情報の発行を受けた前記第1の端末が、前記第2の端末に対して、前記第1の端末の公開情報として、前記第1の端末の公開値yと識別情報iを、前記通信ネットワークを介して転送する端末公開情報転送部と、

前記第1の端末から前記端末公開情報の転送を受けた前記第2の端末が、前記第1の端末の公開鍵として、前記センターの公開情報Yと、前記第1の端末の公開値yと、前記第1の端末の識別情報iを前記公開鍵生成関数Pに入力したときの出力値

$$C = P(Y, y, i)$$

を生成する公開鍵生成部から構成されることを特徴とした公開鍵生成システム。

(6) 請求項5記載の公開鍵生成システムにおいて、

qを素数もしくは素数のべき乗値とし、gを前記qを法とする剰余体の原始元とし、uを前記剰余体のある元としたとき、前記一方向性関数Fとして、前記qを法とし、前記uを入力とする前記gのべき乗剰余値

$$v = F(u) = g^u \bmod q$$

を出力する関数を使用し、ϕを前記qのオイラー関数値としたとき、前記秘密鍵生成関数Sとして、前記ϕを法とし、センターの秘密鍵Xと第1の端末の公開値yの積と、センターの生成した乱数値kと第1の端末の識別情報iの積との和

$$x = S(X, y, k, i) = X \times y + k \times i \bmod \phi$$

を出力する関数を使用し、前記公開鍵生成関数Pとして、前記qを法とし、前記第1の端末の公開値yをべきとした前記センターの公開情報Yのべき乗剰余値と、前記第1の端末の識別情報iをべきとした前記第1の端末の公開値yのべき乗剰余値との積

$$C = P(Y, y, i) = (Y^v) \times (y^i) \bmod q$$

を出力する関数を使用することを特徴とする公開鍵生成システム。

(7) 請求項5記載の公開鍵生成システムにおいて、

qを素数もしくは素数のべき乗値とし、gを前記qを法とする剰余体の原始元とし、uを前記剰余体のある元としたとき、前記一方向性関数Fとして、前記qを法とし、前記uを入力とする前記gのべき乗剰余値

$$v = F(u) = g^u \bmod q$$

を出力する関数を使用し、ϕを前記qのオイラー関数値としたとき、前記秘密鍵生成関数Sとして、前記ϕを法とし、前記第1の端末の公開値yと前記第1の端末の識別情報iをある公開の関数Hに入力したときに得られる出力値hと、前記センターの秘密鍵Xの積と、前記センターの生成した乱数値kとの和

$$x = S(X, y, k, i) = H(y,i) \times X + k \bmod \phi = h \times X + k \bmod \phi$$

を出力する関数を使用し、前記公開鍵生成関数Pとして、前記qを法とし、前記第1の端末の公開値yと前記第1の端末の識別情報iを前記関数Hに入力したときに得られる出力値hをべきとした前記センターの公開情報Yのべき乗剰余値と、前記第1の端末の公開値yとの積

$$C = P(Y, y, i) = (Y^{H(y,i)}) \times y \mod q = (Y^{h}) \times y \mod q$$

を出力する関数を使用することを特徴とする公開鍵生成システム。

(8) 請求項5記載の公開鍵生成システムであって、前記端末情報の発行ステップの後に、前記第1の端末が、検証用公開鍵として、前記第1の端末の秘密鍵xを前記一方向性関数Fに入力したときの出力値V＝F（x）を生成する検証用公開鍵生成ステップを追加し、

前記端末公開情報転送ステップにおいて、前記第1の端末が、前記第2の端末に、前記検証用公開鍵Vと、前記第1の端末の識別情報iと、前記第1の端末の公開値yを、前記第1の端末の公開情報として前記通信ネットワークを介して転送し、

前記第1の端末から端末公開情報の転送を受けた前記第2の端末が、前記公開鍵生成ステップの後に、前記公開鍵生成ステップで生成された前記第1の端末の公開鍵Cと前記検証用公開鍵Vを比較し、一致するか否かを確認する公開鍵確認ステップを追加することを特徴とした公開鍵生成システム。

3．発明の詳細な説明

産業上の利用分野

本発明は、複数の端末と端末情報発行センターからなるシステムにおいて、各端末が、センターの公開情報と相手の端末の公開情報を用いて、相手端末の公開鍵を生成する方式およびシステムに関する。

従来の技術

公開鍵を利用した相手認証、暗号通信、鍵配送、および署名などのプロトコル（以下では単に公開鍵暗号系プロトコルと称する）は、大規模のネットワークに適しているため、近年特に注目を浴びている。しかし、公開鍵暗号系プロトコルでは、公開鍵の完全性、すなわち、その公開鍵がまさに当該の端末のものであるということが保証されなければならない。公開鍵の完全性を保証する手段として、信頼のおけるセンターが公開鍵を管理する方法と、各端末がそれぞれの公開鍵を自分で管理し、暗号プロトコルの開始に先だって、相手端末から公開鍵を配送してもらう方法がある。

前者は、端末数の多い大規模ネットワークに使用する場合、センターへのアクセスが集中し、センターの鍵管理の負担が大きくなるという問題点がある。

一方、後者は、センターの負担が軽減される反面、その公開鍵の完全性を保証するために、センター発行の署名情報（証明書と呼ばれることがある）を必要とし、端末はその署名情報を用いて公開鍵の完全性を確認しなければならない。

以上の方法とは別に信頼のおけるセンターが各端末の秘密鍵と公開可能な数値（以下では単に公開値と称する。この公開値は秘密鍵に対応する公開鍵そのものではない）を、端末情報として発行し、この端末情報を用いて相手認証を行なうプロトコルが、ベスによって、提案されている。このベスの方式は、公開値の完全性確認を単独では行わず、相手端末を認証する時に同時に、公開値の完全性確認を行なう方式とみることができる。ただしこの方式では相手認証プロトコルのみに限定される。

ここでは、まずセンター発行の署名情報を用いて公開鍵の完全性を確認する方法の一例としてエルガマル署名法を用いた方法について述べ、次に、ベスの提案した相手認証の方式について述べる。なお、エルガマル署名法は離散対数問題の難しさをもとにした署名法で、"ア パブリック キー クリプトシステム アンド ア シグニチャスキーム ベイスト オン ディスクリート ログリズムズ"アイイーイーイー トランザクション オン インフォメイション セオリ(T.E.ElGamal:"A public key cryptosystem and a signator

e scheme based on discrete logarithms", IEEE Trans. on IT, vol.IT-31.NO.4 PP469-472)に詳しい。また、ベスの方式は、"エフィシェント ゼロナレッジ アイデンティフィケーション スキーム フォ スマートカード"ユーロクリプト'88 (Beth:"Efficient zero-knowledge identification scheme for smart cards" Lect Notes Comput Sci VOL330 P77-84 '88)に詳しい。

[従来例1]

ここでは、各端末が、各自の公開鍵を管理し、その公開鍵の完全性をセンター発行の署名情報で保証する方法について述べる。なお完全性の確認された公開鍵を用いて、任意の公開鍵暗号系プロトコルを実現できる。以下では、1)システム初期設定、2)端末の鍵生成、3)署名情報の発行請求、4)署名情報の発行、5)公開鍵の完全性確認の各ステップの順に述べる。なお、1)から4)の各ステップは端末がこのシステムに加入する時に一度だけ実行されるステップである。

1)システム初期設定

センターは以下の手順でシステムの初期設定を行なう。

(1)大きな素数もしくは素数のべき乗値qと、GF(q)の原始元gを公開する。

ここで、GF(q)はqを法とする有限体を示す。

(2)センターの秘密鍵Xを決め、

$$Y=g^X \bmod q \qquad (1.1)$$

で定まるY をセンターの公開鍵として公開する。

ここでmodqはq で除したときの剰余の算出を示す。また式(1.1) において、入力値X から出力値Y を求めることは容易であるが、出力値Y から入力値X を求めることは離散対数問題に依存し困難である。このような性質を満たす関数は一方向性関数と呼ばれる。

2)端末の鍵生成

端末i は秘密鍵xiを決定し、xiに対応する公開鍵

$$yi=g^{xi} \bmod q \qquad (1.2)$$

を決定する。

3)署名情報の発行請求

端末iは、公開鍵yiと端末i の識別情報IDi を、端末の公開情報として、センターに通知し、センターの署名情報の発行を請求する。

なお、識別情報は名前や住所などの端末固有の公開情報である。なお、以降の変数における添字i は任意の端末i 用の変数であることを示す。

4)署名情報の発行

センターは、端末iから受け取った端末の公開情報 (yi,IDi) に対して、エルガマル署名法を使ってセンター署名情報を発行する。センターによる署名情報の発行手順は以下のとおりである。

(1)センターはなんらかの手段で端末i の正当性を確認する。

(2)乱数kiを発生する。

(3)エルガマル署名法を用いて、端末iの公開情報 (識別情報IDi と公開鍵yi) に対する署名情報(ti,ui)

$$ti=g^{ki} \bmod q \qquad (1.3)$$

$$ui=(yi::IDi-X\times ti)/ki \bmod \phi \qquad (1.4)$$

(' :: はデータの連結を示す。)

を生成し、端末i に発行する。

ここでϕは、qのオイラー関数値を示す。オイラー関数については、例えば "暗号と情報セキュリティ"の第1章:基礎数学 (昭晃堂) に詳しい。なお、発行される署名情報(ti,ui) は公開可能な情報であり、端末へは磁気カードなどを媒体として発行される。

5)公開鍵の完全性確認

ここでは、端末j が端末i の公開鍵の完全性を確認する場合について述べる。

(1)端末j は、端末i より端末iの公開情報 (yi,IDi) とセンター発行の署名情報(ti,ui)を受け取る。

(2)端末j は、受け取った端末i の公開情報 (yi,IDi) とセンター発行の署名情報(ti,ui)が

$$g^{(yi::IDi)}=yi^{ti}\times ti^{ui} \bmod q \qquad (1.5)$$

を満たすかどうか検査し、式(1.5) が成立する場合に、公開鍵yiがまさに端末iの公開鍵であると認識する。

この従来例によれば、次の(1) ～(4) に列挙のような特徴がある。

(1) 各端末が各自の秘密鍵x と公開鍵yiを生成し、端末の公開情報（公開鍵yiと識別情報IDi ）に対する署名情報をセンターが発行する。

(2) 各端末は、相手端末の公開情報（yi,IDi）とセンター発行の署名情報（ti,ui ）を用いて、相手端末の公開鍵の完全性を確認する。

(3) 完全性の確認された公開鍵を用いて任意の離散対数演算ベースの公開鍵暗号系プロトコルを構成できる。

(4) 公開鍵の完全性確認に、modq上のべき乗剰余演算を３回行う必要がある。

［従来法２］

ベスが提案した相手認証プロトコルは、センターの公開情報と、端末の公開情報（端末の識別情報とセンター発行の公開値）を用いて相手の認証を行なう方式である。なお、端末の秘密鍵と公開値は、センターが発行する。以下では、上述のベスの文献において推奨されている方式について、1)システム初期設定、2)端末情報の発行請求、3)端末情報の発行、4)相手端末の認証の各ステップの順に述べるが、1)から3)の各ステップは端末がこのシステムに加入する時に一度だけ実行されるステップである。

1)システム初期設定

センターは以下の手順でシステムを構成する。

(1)大きな素数または素数のべき乗値q とGF(q) の原始元g を公開する。

(2)センターの秘密鍵X を決め、

$$Y=g^{X} \mod q \qquad (2.1)$$

を公開する。

2)端末情報の発行請求

端末i は、識別情報IDi をセンターに通知し、端末情報として端末の秘密鍵xiと公開値yiの発行を請求する。

3)端末情報の発行

センターは、端末情報の発行を以下の手順で行なう。

(1)センターはなんらかの手段で端末i の正当性を確認する。

(2)乱数kiを発生する。

(3)エルガマル署名法を用いて、識別情報IDi に対する署名情報(yi,xi)

$$yi=g^{ki} \mod q \qquad (2.2)$$

$$xi=(IDi-X\times yi)/ki \mod \phi \qquad (2.3)$$

を生成し、xiは端末の秘密鍵として、yiは端末の公開値として、端末i に発行する。

なお、端末の秘密鍵xiは、ICカードなどの物理的に安全なメモリを媒体として発行される。

4)相手端末の認証

端末i が端末j に自分の正当性を証明する場合について説明する。

(1)端末i は、端末j に端末の公開情報として、識別情報IDi および端末の公開値yiを送付する。

(2)端末j は受け取った（IDi,yi）を用いて

$$\rho i = y^{yi} \mod q \qquad (2.4)$$

を得る。

(3)端末i は、乱数Ri を用いて

$$C1=yi^{Ri} \mod q \qquad (2.5)$$

を計算し、端末j に送付する。

(4)端末j は、乱数E を端末i に送付する。

(5)端末i は、自身の秘密鍵xiを用いて、

$$C2=E\times xi+Ri \mod \phi \qquad (2.6)$$

を計算し、端末j に送付する。

(6) 端末j は、$v=E\times IDi \mod \phi$ を求め

$$\rho^{E}\times y^{C2}\times C1=g^{v} \mod q \qquad (2.7)$$

が成立するかどうかを検査し、式(2.7)が成り立つ場合に、相手端末が、まさに端末i であると認識する。

この従来例によれば、次の(1) ～(4) に列挙する特徴がある。

(1) センターが、各端末に対して、各端末の秘密鍵と端末の公開値を生成する。

(2) 各端末は、センターの公開情報と相手端末の公開情報（公開値yiと識別情報IDi ）を用いて、相手端末の認証を行う。

(3) 任意の離散対数演算ベースの公開鍵暗号系プロトコルを構成できない。

(4) 相手認証時に、modq上のべき乗剰余演算を

3回行う必要がある。

発明が解決しようとする課題

ところで、従来例1によれば、相手端末の公開鍵の完全性は、相手端末の公開情報（yi,IDi）とセンター発行の署名情報（ti,ui）を用いなければ確認できないし、また、その確認にmodq上のべき乗剰余演算を3回も行なわねばならず、計算量が大変多いという課題がある。

一方、従来例2によれば、任意の離散対数演算ベースの公開鍵暗号系プロトコルを構成できないし、相手認証時に、modq上のべき乗剰余演算を3回行わねばならず、やはり計算量が多く煩瑣であるという課題がある。

本発明はこのような点にあって、生成された公開鍵を用いて任意の離散対数演算ベースの公開暗号系プロトコルを構成できると共に、公開鍵の完全性の確認をあえて行う必要がなく、また、べき乗剰余演算の計算量を少なくすることのできる公開鍵生成方式および公開鍵生成システムを提案することを目的としている。

課題を解決するための手段

上記目的を達成するため、本発明は、端末情報発行センターが、センターの秘密鍵Xと、ある秘密鍵生成関数Sを有し、ある一方向性関数Fと、ある公開鍵生成関数Pと、前記秘密鍵Xを一方向性関数Fに入力したときの出力値Y＝F（X）を、第1および第2の端末に通知する初期設定ステップと、

第1の端末が端末情報発行センターに、第1の端末固有の識別情報iを通知し、端末情報の発行を請求する端末情報発行請求ステップと

端末情報発行センターが、ある乱数値kを前記一方向性関数Fに入力したときの出力値y＝F（k）を生成し、センターの秘密鍵Xと、端末の公開値yと、乱数値kと、端末の識別情報iを秘密鍵生成関数Sに入力したときの出力値xを生成し、前記yと前記xを端末に発行する端末情報発行ステップと、

第1の端末が、第2の端末に、端末の識別情報iと端末の公開値yを転送する端末公開情報転送ステップと、

第2の端末が、センターの公開情報Yと、第1の端末の公開値yと、第1の端末の識別情報iを公開鍵生成関数Pに入力したときの出力値Cを生成する公開鍵生成ステップを備えたものである。

また、端末情報発行センターが、qを素数もしくは素数のべき乗値とし、gをqを法とする剰余体の原始元とし、uを前記剰余体の元としたとき、前記qを法とし、前記uを入力とする前記gのべき乗剰余値

$$v = g^u \mod q$$

を出力する一方向性関数Fと、qのオイラー関数値ϕを法とし、センターの秘密鍵Xと第1の端末の公開値yの積と、センターの生成した乱数値kと第1の端末の識別情報iの積との和

$$x = X \times y + k \times i \mod \phi$$

を出力する秘密鍵生成関数Sと、qを法とし、第1の端末の公開値yをべきとしたセンターの公開情報Yのべき乗剰余値と、第1の端末の識別情報iをべきとした前記第1の端末の公開値yのべき乗剰余値との積

$$C = (Y^y) \times (y^i) \mod q$$

を出力する公開鍵生成関数Pを備えたものである。

また、端末情報発行センターが、第1の端末の公開値yと第1の端末の識別情報iをある定められた関数Hに入力したときに得られる出力値hと、センターの秘密鍵Xの積と、センターの生成した乱数値kとの和

$$x = H(y,i) \times X + k \mod \phi$$
$$= h \times X + k \mod \phi$$

を出力する秘密鍵生成関数Sと、前記qを法とし、第1の端末の公開値yと第1の端末の識別情報iを前記関数Hに入力したときに得られる出力値hをべきとしたセンターの公開情報Yのべき乗剰余値と、前記第1の端末の公開値yとの積

$$C = (Y^{H(y,i)}) \times y \mod q$$
$$= (Y^h) \times y \mod q$$

を出力する公開鍵生成関数Pを備えたものである。

また、第1の端末が、検証用公開鍵として、第1の端末の秘密鍵xを一方向性関数Fに入力したと

きの出力値Ｖ＝Ｆ（ｘ）を生成する検証用公開鍵生成ステップと、第１の端末が、第１の端末の識別情報ｉと第１の端末の公開値ｙと検証用公開鍵Ｖを第２の端末に転送する端末公開情報転送ステップと、

第２の端末が、公開鍵生成ステップで得た第１の端末の公開鍵Ｃと前記Ｖを比較し、一致するか否かを確認する公開鍵確認ステップを備えたものである。

作用

本発明による公開鍵生成方式では、上述の構成によって、第２の端末は、センターの公開情報Ｙと、第１の端末から受け取った端末の公開情報（公開値ｙと識別情報ｉ）を用いて、第１の端末の公開鍵の生成を行なう。端末の公開鍵の生成に、センター発行の公開情報を用いるため、あえて公開鍵の完全性を独立に確認する必要はない。

また、特許請求の範囲第２項記載の構成によって、各端末が相手端末の公開鍵生成に必要な計算量を、べき乗剰余演算２回にすることが可能である。また特許請求の範囲第３項記載の構成によって、さらに計算量をべき乗剰余演算１回に削減可能である。

また特許請求の範囲第４項記載の構成によって、公開鍵の完全性の確認を独立に行なうことも可能としている。

実施例

第１図は本発明の第１の実施例におけるシステム構成の概略を示すものであって、10は端末情報発行センター、20は第１の端末、30は第２の端末、40はセンターと端末間で設定されている通信路、50は第１の端末と第２の端末間で設定されている通信路である。

第２図は本発明の第１の実施例による鍵生成方式における、1)システム初期設定ステップ、2)端末情報請求ステップ、3)端末情報発行ステップの各ステップの概略を示し、第３図は、4)端末情報転送ステップ、5)公開鍵生成ステップの各ステップの概略を示している。

次に第１の実施例における鍵生成方式の動作について

ついて第２図および第３図を使って詳細に説明する。

1)システム初期設定ステップ

センターは以下の手順でシステムを構成する。

(1)大きな素数または素数のべき乗値ｑとGF(ｑ)の原始元ｇを生成し、ｑを11の法格納部に、ｇを12の原始元格納部に格納する。

(2)センターの秘密鍵Ｘを決定し、13の秘密鍵格納部に格納し、14の一方向性関数Ｆにセンターの秘密鍵Ｘを入力して

$$Y = F(X) = g^X \bmod q \quad (1)$$

を生成する。（ｑ,ｇ,Ｙ）と公開鍵生成ステップにおいて使用する公開鍵生成関数Ｐをセンターの公開情報として各端末に公開する。

2)端末情報請求ステップ

端末ｉは21の識別情報格納部に格納された端末ｉ固有の識別情報ＩＤｉを41の端末情報の請求用の通信路を通じて、センターに通知し、端末情報の発行を請求する。なお、41の端末情報の請求用の通信路は、相手端末の正当性を確認できる通信路（認証可能な通信路）であるとする。

3)端末情報発行ステップ

端末ｉからの端末情報発行の請求に対して、センターは端末情報の発行を以下の手順で行なう。

(1)センターは端末ｉの正当性を確認する。

(2)15の乱数生成装置を用いて乱数ｋｉを発生する。

(3)乱数ｋｉを14の一方向性関数に入力して端末の公開値

$$y_i = g^{k_i} \bmod q \quad (2)$$

を生成し、センターの秘密鍵Ｘと端末ｉの公開値ｙｉと乱数ｋｉと端末ｉの識別情報ＩＤｉを16の第１の秘密鍵生成関数Ｓに入力して端末の秘密鍵

$$x_i = S(X, y_i, k_i, ID_i) = X \times y_i + k_i \times ID_i \bmod \phi \quad (3)$$

を生成し、42の端末情報発行用通信路を通じて端末ｉに発行する。ここでφはｑのオイラー関数値を示す。

なお、42の端末情報発行用通信路は、外部に対して安全な通信路とする。例えばＩＣカードなどの

物理的に安全なメモリを媒体とする。

以上のステップは端末がこのシステムに加入するときに一度だけ実行されるステップである。

4)端末公開情報転送ステップ

端末i は、端末j に、21の格納部に格納された識別情報IDiと22の格納部格納されたセンター発行の端末i の公開値yiを、51の端末情報転送用通信路を通じて送付する。

5)公開鍵生成ステップ

端末j は、受け取った (IDi,yi) を、31の第1の公開鍵生成関数Pに入力して、端末iの公開鍵

$$Pi = P\ (V,yi,IDi) = (V^{yi}) \times (yi^{IDi}) \bmod q \qquad (4)$$

を生成する。

このようにして、センターの公開情報と端末の公開情報を用いて、相手端末の公開鍵を生成する。なお上述の手順で、相手端末の公開鍵を生成したのち、次のステップとして、その公開鍵を用いて、さまざまな公開鍵暗号系プロトコルが実現できる。ここでは、一例として相手認証プロトコルの例について以下で述べるが、他の公開鍵を用いた暗号プロトコルに置き換えることもできる。

ここで示す相手認証プロトコルは、チャウムと木崎によって提案された相手認証方式をもとにし構成される例であり、第6図に概略を示す。なお、チャウムと木崎が提案した認証方式については、"アン インプルーブド プロトコル フォー デモンストレーティング ポゼッション オブ ディスクリート ロガリズムズ アンド サム ジェネラリゼイションズ"ユーロクリプト87(D.Chaum:"An improved protocol for demonstrating possession of discrete logarithms and some generalizations",EUROCRYPT87)、または、"アノート オン ゼロノレジ プルーフ フォー ザ ディスクリート ロガリズム プロブレム"、ザ トランザクション オブ ザ アイイーアイシーイー1988(K.Kizaki:"A note on zero-knowledge proof for the discrete logarithm problem",The Trans.of the IEICE,Vol.E71,No.1,January,1988)に詳しい。

端末i が端末j に自分の正当性を証明する場合について説明する。なお端末j は、既に端末i の公開鍵Piを上述の手順で生成しているものとする。

6)相手認証ステップ

(1) 端末i は、乱数Ri を発生し、

$$C1 = g^{Ri} \bmod q$$

を計算し、端末 j に送付する。

(2) 端末j は、乱数E を端末i に送付する。

(3) 端末i は、自身の秘密鍵xiを用いて、

$$C2 = E \times xi + Ri \bmod \phi$$

を計算し、端末j に送付する。

(4) 端末j は、検証式

$$g^{C2} = (Pi^{E}) \times C1 \bmod q$$

が成立するか否かを検査し、検証式が成り立つ場合には相手端末がまさに端末iであると認識する。

上記第1の実施例における特徴は以下のとおりである。

(1) センターが、各端末に対して、各端末の秘密鍵 x と端末の公開値yi (公開鍵ではない) を生成する。

(2) 各端末は、センターの公開情報Vと相手端末の公開情報 (公開値yiと識別情報IDi) を用いて、相手端末の公開鍵Piを生成する。

(3) 生成された公開鍵Piを用いて、任意の離散対数演算ベースの公開鍵暗号系プロトコルを構成できる。

(4) 公開鍵の生成に必要となる計算量は、modq 上のべき乗剰余演算2回である。なお、端末iが自身の秘密鍵xiを用いて、自分の公開鍵

$$Vi = g^{xi} \bmod q$$

を求め、端末j に送付し、端末j はViを第1の公開鍵生成関数Pで求めた公開鍵Piと比較することによって公開鍵の完全性を単独に確認することもできる。

また、第1の秘密鍵の生成関数を次式の関数に置き換えてもよい。

$$xi = S\ (X,yi,ki,IDi) = X \times IDi + yi \times ki \bmod \phi$$

この時、第1の公開鍵生成関数は、

$Pi = P(Y, yi, IDi) = (Y^{hash(IDi, yi)}) \times (yi^{yi}) \bmod q$

となる。

第4図は本発明の第2の実施例による鍵生成方式における、1)システム初期設定ステップ、2)端末情報請求ステップ、3)端末情報発行ステップの各ステップの概略を示し、第5図は、4)端末情報転送ステップ、5)公開鍵生成ステップの各ステップの概略を示している。

次に第2の実施例における鍵生成方式の動作について第4図および第5図を使って詳細に説明する。この実施例は、第1の実施例にハッシュ関数を導入することによって、公開鍵生成における計算量を削減するものである。なお、ハッシュ関数の計算量はべき乗剰余演算に比べて極めて小さいとしている。

1)システム初期設定ステップ

センターは以下の手順でシステムを構成する。

(1)大きな素数または素数のべき乗値qとGF(q)の原始元gを生成し、qを11の法格納部に格納し、gを12の原始元格納部に格納する。

(2)センターの秘密鍵Xを決定し、13の秘密鍵格納部に格納し、14の一方向性関数Fにセンターの秘密鍵Xを入力して

$$Y = F(X) = g^X \bmod q \quad (5)$$

を生成する。

(3)ハッシュ関数hash( )を決定し、公開する。ここでハッシュ関数とは、複数の入力データに対してそれらに依存した圧縮データを出力する関数のことである。センターの公開情報として(q, g, Y)と、ハッシュ関数hash( )と、公開鍵生成ステップにおいて使用する公開鍵生成関数Pを各端末に公開する。

2)端末情報請求ステップ

端末i は21の識別情報格納部に格納された端末i固有の識別情報IDiを41の端末情報の請求用の通信路を通じて、センターに通知し、端末情報の発行を請求する。なお、41の端末情報の請求用の通信路は、相手端末の正当性を確認できる通信路(認証可能な通信路)であるとする。

3)端末情報発行ステップ

端末i からの端末情報発行の請求に対して、センターは端末情報の発行を以下の手順で行なう。

(1)センターは端末i の正当性を確認する。

(2)15の乱数生成装置を用いて乱数kiを発生する。

(3)乱数kiを14の一方向性関数に入力して端末の公開値

$$yi = g^{ki} \bmod q \quad (6)$$

を生成し、識別情報IDiと乱数kiとセンターの秘密鍵Xと端末の公開値yiを17の第2の秘密鍵生成関数Sに入力して端末の秘密鍵

$$xi = S(X, yi, ki, IDi) = hash(IDi, yi) \times X + ki \bmod \phi$$
$$= X \times hi + ki \bmod \phi \quad (7)$$

を生成し、42の端末情報発行用通信路を通じて端末i に発行する。ここでϕはqのオイラー関数値を示す。

なお、42の端末情報発行用通信路は、外部に対して安全な通信路とする。例えばICカードなどの物理的に安全なメモリを媒体として発行することにより実現する。

以上のステップは端末がこのシステムに加入するときに一度だけ実行されるステップである。

4)端末公開情報転送ステップ

端末i は、端末j に、21の識別情報格納部に格納された識別情報IDiと22の格納部格納されたセンター発行の端末i の公開値yiを、51の端末情報転送用通信路を通じて送付する。

5)公開鍵生成ステップ

端末j は、受け取った(IDi, yi)を、32の第2の公開鍵生成関数Pに入力して、端末iの公開鍵

$$Pi = P(yi, IDi, Y) = Y^{hash(IDi, yi)} \times yi \bmod q$$
$$= (Y^{hi}) \times yi \bmod q \quad (8)$$

を生成する。

このようにして、センターの公開情報と端末の公開情報を用いて、相手端末の公開鍵を生成する。なお上述の手順で、相手端末の公開鍵を生成したのち、第1の実施例と同様に、次のステップとし

て、その公開鍵を用いて、さまざまな公開鍵暗号系プロトコルが実現できる。

以上の第2の実施例における特徴は、第1の実施例の（1）～（4）の特徴に加え、（5）公開鍵生成までの計算量が、べき乗剰余演算1回とハッシュ関数の演算1回で済むという点もある。

なお、端末iが自身の秘密鍵xiを用いて、自分の公開鍵

$$Vi=g^{xi} \mod q$$

を求め、端末j に送付し、端末j は、このViと、第2の公開鍵生成関数Pを用いて生成した公開鍵Piを比較することによって公開鍵の完全性を単独に確認することもできる。

また、第2の秘密鍵の生成関数を次式の関数に置き換えてもよい。

$$xi = S\ (X,yi,ki,IDi) = X + hash(IDi,yi) \times ki \mod \phi$$
$$= X + hi \times ki \mod \phi$$

この時、第2の公開鍵生成関数は、

$$Pi = P\ (Y,yi,IDi) = Y \times yi^{hash(IDi,yi)} \mod q$$
$$= Y \times (yi^{hi}) \mod q$$

となる。

発明の効果

以上の説明から明らかなように本発明は、各端末が、センターの公開情報と、相手端末の公開情報（センター発行の端末の公開値と端末の識別情報）を用いて、公開鍵を生成する方式であるので、本発明による公開鍵生成方式で生成した公開鍵を用いれば、相手認証、暗号通信、署名などの公開鍵暗号系プロトコルを実現できると共に、その場合、従来独立に必要であった公開鍵の完全性確認のステップを省略することができるという効果がある。また、各端末が各自の秘密鍵を用いて直接生成した検証用公開鍵と、各端末が、相手端末の公開情報から生成した公開鍵を比較することで、公開鍵の完全性確認を独立に行なうことも可能であるという効果もある。

単に、公開鍵の生成に必要な計算量が、従来の技術ではべき乗剰余演算3回であったが、本発明では、べき乗剰余演算2回に削減でき、さらにハッシュ関数を導入することによって、べき乗剰余演算1回に削減している。

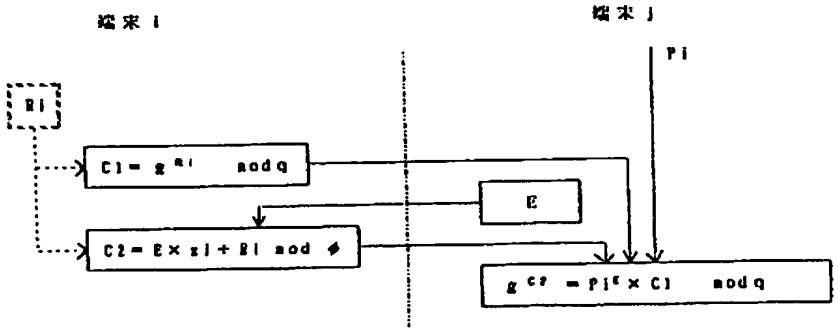
なお、本発明においては端末の秘密鍵はセンターが生成するので、センターから端末への配送には物理的安全性が保証されたICカードなどの媒体を用いることが必要である。

4．図面の簡単な説明

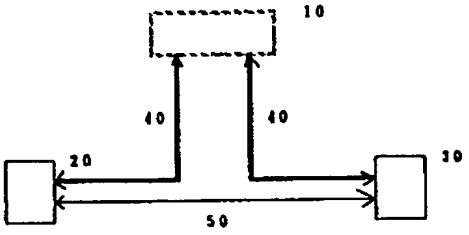
第1図は本発明の第1の実施例による鍵生成方式のシステムの構成図。第2図は本発明の第1の実施例の構成図（1）。第3図は本発明の第1の実施例の構成図（2）。第4図は本発明の第2の実施例の構成図（1）。第5図は本発明の第2の実施例の構成図（2）。第6図は従来の技術による相手認証プロトコル。

10…端末情報発行センター、20…第1の端末、30…第2の端末、40…センター・端末間通信路、50…第1の端末・第2の端末間通信路、11…法格納部、31…第1の公開鍵生成関数、12…原始元格納部、32…第2の公開鍵生成関数、13…秘密鍵格納部、41…端末情報発行請求用通信路、14…一方向性関数、42…端末情報発行用通信路、15…乱数生成装置、51…端末情報転送用通信路、16…第1の秘密鍵生成関数、17…第2の秘密鍵生成関数、22…公開値格納部、21…識別情報格納部。

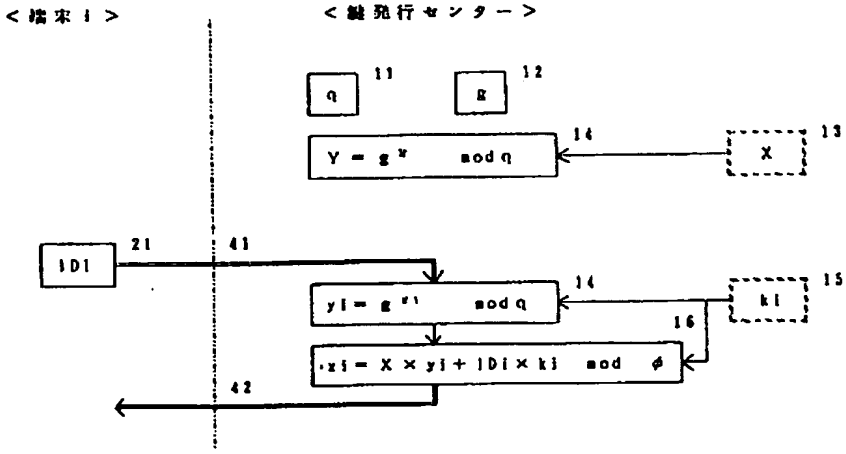
代理人　弁理士　中島司朗



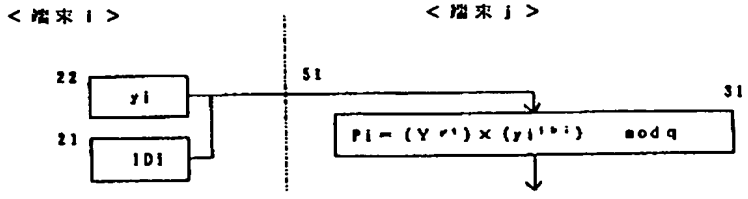
第6図　相手認証プロトコル



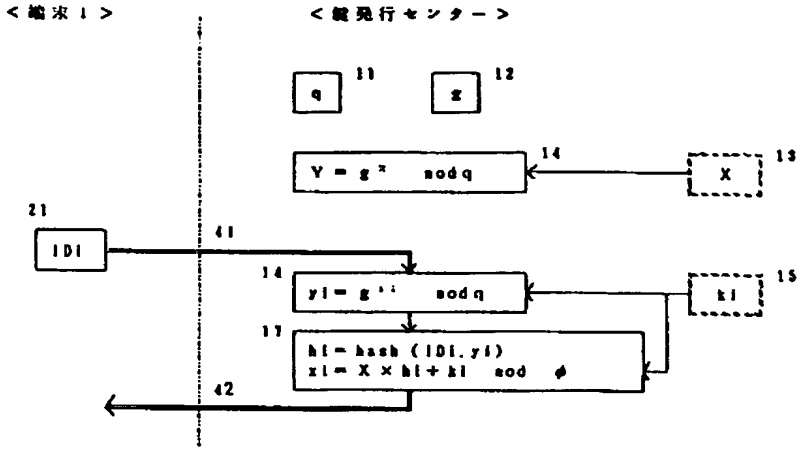
第1図　システム構成



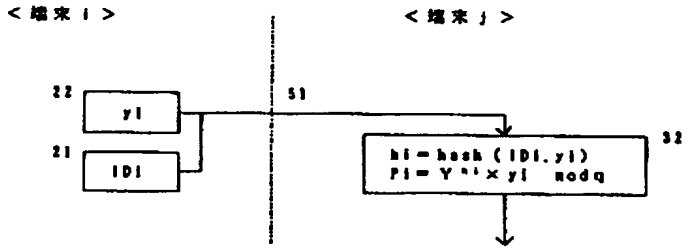
第2図　第1の実施例の構成図（1）



第3図　第1の実施例の構成図（2）



第4図　第2の実施例の構成図（1）



第5図　第2の実施例の構成図（2）